Sandy Bacik

From: Sandy Bacik
Sent: Friday, February 03, 2012 6:39 AM
To: csctgarchi@nist.gov
Subject: CSWG Architecture minutes from 20120202

CSWG Architecture twiki: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGArchi
Chair: Sandy Bacik (sandy.bacik@enernex.com)

20120202 Minutes

1. A summary pdf of the conceptual security architecture consensus work can be found here:
   https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Conceptual_Security_Architecture_-_Consensus_Progress.pdf.
2. Conceptual security architecture - applying security services (http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/20120202-SecurityServicesToMessages.ppt).
   a. Slide 1-2. We discussed a drawing showing that messages can cross domain and cross information classifications. The drawing has improved, but it needs a legend and description for what it is showing. Sandy will update the drawing with a legend and description for our next call. Elizabeth Sisley sent a comment to the list about the drawing and this will be corrected for our next meeting.
   b. Slide 3. We discussed putting an architecture type roadmap drawing into the updated NISTIR to show where the conceptual security architecture fit into an over architecture development process. Sandy will validate the source of the drawing or if it was designed from scratch and note the source.
   c. Slide 4. We discussed a flow diagram to show that we will be focusing on messages and security services for the conceptual security architecture, but we couldn't determine an easy way to integrate the spaghetti drawing work. Additional consideration will be needed for this drawing.
   d. Slide 6. The initial outline for the conceptual security architecture was drafted and needs to be refined in the future meetings.
   e. Slide 10. User Interface for Security: Enterprise, SG Component, SG Application - Yes; all messages - No.
   f. Slide 11. User Support: Enterprise, SG Component, SG Application - Yes; all messages - No.
   g. Slide 12. We listed the security services that will apply to all messages based on previous meetings.
   h. We has consensus on specific security services that would not apply to ANY message.
      i. The security services that would not apply to ANY message are Certification - Enterprise Credentials, Certification - Enterprise Public Key, Certification and Accreditation, Environmental Security, Personnel Security, Replication and Backup - Software
      ii. We did not have consensus on the following security services that would not apply to ANY message: Integrity Protection - Hardware, Integrity Protection - Software, Physical Security, Software Licensing
   i. We started a discussion on applying specific security services to message types and if we should apply the services at all C-I-A levels or assign C-I-A levels to message types and then proceed with assigning the security services.
      i. Sandy will describe in detail how PAP2 proceeded with developing their transaction spreadsheet for wireless technologies in our next call.
      ii. Sandy will discuss potential options we can use for assigning security services to the last 23 message types for the last 20 security services.
3. Open Items.
   a. When do our updates need to be completed? We should have a draft update of the NISTIR 7628 chapter 2 content and the conceptual security architecture completed by April 25 for the CSWG F2F in Sterling, VA at Neustar headquarters.
   b. A question was asked if the DNP3 (IEEE 1815) message types maps to our message types. Yes, they do and Sandy will try to get the mapping ready to display for our next call.
4. Attendees.
   a. Daniel Friedman

b. Elizabeth Sisley
   c. Rich Tolway
   d. Sandy Bacik

Regards,
Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant
EnerNeX
p: 865.696.4470
e: sandy.bacik@enernex.com // www.enernex.com